Department of Homeland Security
Daily Open Source Infrastructure Report for 8 January 2008

Current Nationwide

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here

- The Associated Press reported that hundreds of thousands of Californians were still without power after a series of fierce storms pounded the state over the weekend and toppled nearly 500 miles of power lines. More than 145,000 homes and businesses in Northern California and the Central Valley were in the dark Sunday, down from more than 215,000 earlier in the day, ahead of rain and snow that were forecast to return again soon. In all, more than 2 million customers from the Oregon border to Los Angeles have lost power since the storms arrived Friday. (See items **1**)
- According to Computer Weekly, hackers may be able to access aircraft flight and management systems in Boeing's new mid-range jet, the 787-8. The FAA said that there are links between the networks that run the passenger "domain," which allows passengers to access the internet during flights, and aircraft-management systems. A Boeing spokesman said the aircraft maker was aware of the problem and would test its fix in March. (See item **11**)

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: **Energy; Chemical; Nuclear Reactors, Materials and Waste; Defense Industrial Base; Dams**

Service Industries: **Banking and Finance; Transportation; Postal and Shipping; Information Technology; Communications; Commercial Facilities**

Sustenance and Health: **Agriculture and Food; Water; Public Health and Healthcare**

Federal and State: **Government Facilities; Emergency Services; National Monuments and Icons**

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) – [http://www.esisac.com]

1. *January 7, Associated Press* – (California) **Many without power for days as rain, snow continue in California.** Hundreds of thousands of Californians were still without

power after a series of fierce storms pounded the state over the weekend and toppled nearly 500 miles of power lines. More than 145,000 homes and businesses in Northern California and the Central Valley were in the dark Sunday, down from more than 215,000 earlier in the day, ahead of rain and snow that were forecast to return again soon. A meteorologist with the National Weather Service said some parts of Northern California would get a reprieve from the rain and snow on Monday. But in the mountains, “there’s a chance of snow and snow showers all the way through Thursday,” he said. The storm was expected to weaken in Southern California, with the forecast calling for a 30 percent chance of rain on Monday, the NWS said. Utility crews were using the break in the weather to work on power lines. In all, more than 2 million customers from the Oregon border to Los Angeles lost power since the storms arrived Friday.
Source: http://www.examiner.com/a-1142232~Many_without_power_for_days_as_rain__snow_continue_in_California.html

2. *January 7, Reuters* – (International) **Oil jumps above $98 on new U.S.-Iran tensions.** Oil rose above $98 a barrel before falling back on Monday as reports of rising tensions in the Middle East outweighed concerns of demand outlook in top consumer United States from a feared economic recession. CNN reported that five Iranian Revolutionary Guard boats harassed and provoked three U.S. Navy ships in the Strait of Hormuz on Saturday. Citing unidentified U.S. officials, *CNN* said the Iranian vessels came within 200 yards of the U.S. ships and that after a threatening radio communication, U.S. sailors manned their ships’ guns and were very close to opening fire. Relations between the two countries are already tense over Iran’s nuclear program. Traders said the news had helped put the focus back on geopolitical risks in the oil market.
Source:
http://today.reuters.com/news/articlenews.aspx?type=businessNews&storyid=2008-01-07T144543Z_01_T39048_RTRUKOC_0_US-MARKETS-OIL.xml

[Return to top]

Chemical Industry Sector

3. *January 5, WLWT 5 Cincinnati* – (Ohio) **12 hospitalized after chemical explosion.** In Ohio, several workers from the Sumco Phoenix Corporation spent Saturday morning in the hospital, following a chemical fire at their plant. Firefighters said they were called to the plant at approximately 2:15 a.m. Saturday, when employees reported an explosion. When crews arrived, they said they found multiple hazardous chemicals had spilled onto the ground and generated a reactive explosion and caused high heat. The plant was evacuated and roads in the area were closed for hours while they cleaned up the mess. Plant officials said that a total of 12 workers were brought to the hospital as a precaution. According to a press release, the fire and chemicals were contained inside a room designed to control hazardous-material spills and fires. Firefighters said no chemicals leaked into the air, so neighbors did not need to be evacuated.
Source: http://www.wlwt.com/news/14984443/detail.html

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

4. *January 7, Canadian Press* – (International) **Nuclear body to boost tracking of devices.** Canada's nuclear regulator is changing the way it tracks lost, stolen, and missing nuclear devices following an inquiry about inconsistent reporting from the International Atomic Energy Agency. Newly disclosed internal emails show the Vienna-based agency contacted officials in Ottawa after a Canadian Press investigation raised serious questions in July about how closely the Canadian Nuclear Safety Commission monitors devices that could be used in a crude "dirty bomb." Commission records revealed that dozens of radioactive tools had gone missing in the last five years. Reports of losses or thefts are supposed to be reported to the commission's nuclear security division, which sends case information to the international agency's illicit trafficking database. Established in 1995, the database is intended to be an authoritative global source of information on the unauthorized acquisition, use, and disposal of radioactive material, including accidental losses.
   Source: http://www.thestar.com/article/291561

5. *January 7, Florida Power & Light Company* – (Florida) **St. Lucie Nuclear power plant Unit 2 completes refueling outage.** Florida Power & Light Company's St. Lucie nuclear power plant Unit 2 returned online January 4 following a scheduled refueling and maintenance outage. Unit 2 was taken offline September 30 for its 17th refueling since it began commercial operation in 1983. During refueling outages, scheduled about every 18 months, FPL also performs preventive and scheduled maintenance work that cannot be done when the plant is operating. In addition to routine maintenance and replacement of one-third of the unit's 217 uranium fuel assemblies, workers replaced the unit's two massive steam generators, the reactor vessel head, one of four reactor coolant pump motors, and modified the containment sump system.
   Source: http://biz.yahoo.com/bw/080107/20080107005957.html?.v=1

6. *January 4, Platts* – (National) **NRC issues draft guide on plant security personnel training.** The Nuclear Regulatory Commission has issued a draft regulatory guide on training and qualification of security personnel at nuclear power plants. Released January 4, the draft guide, DG-5015, details a method that NRC staff "considers acceptable." In its introduction, the staff said the guide "describes how licensees should select, train, equip, test, qualify, and requalify armed and unarmed security personnel, watch persons, and other members of the security organization to ensure that these individuals possess and maintain the knowledge, skills, and abilities required to carry out their assigned duties and responsibilities effectively." DG-5015 "is being issued in draft form to involve the public in the early stages of the development of a regulatory position in this area," and "has not received final staff review or approval," the staff said.
   Source:
   http://www.platts.com/Nuclear/News/7771548.xml?sub=Nuclear&p=Nuclear/News&?undefined&undefined

[Return to top]

Defense Industrial Base Sector

7. *January 5, Indianapolis Star* – (National) **Raytheon Technical wins 2 defense contracts.** Raytheon Technical Services has landed two defense contracts worth $41.1 million, the U.S. Defense Department said. A $12.14 million contract for the V-22 Osprey deals with a mission planning system, interactive situational awareness system, desktop test environment, facilities, and simulation for the tilt-rotor aircraft. A $28.99 million award concerns guided missile launchers for the U.S. Navy and Royal Australian Air Force.
   Source:
   http://www.indystar.com/apps/pbcs.dll/article?AID=/20080105/BUSINESS/801050415

[Return to top]

Banking and Finance Sector

8. *January 7, Courier News* – (Illinois) **BBB names top 10 scams.** The Better Business Bureau of Chicago and Northern Illinois has released its top 10 scam list for 2007. In 2006, the list was topped by advance fee lenders, followed by check scams. Those two have reversed for 2007, with check scams now the number 1 scam reported to the bureau. Also, still on this year's list but falling from number 4 to number 9 is the "phishing" scam. While consumers are becoming more aware of this scam and the dangers of identity theft, phishing remains very problematic, and consumers must always be on guard to protect their personal and financial information from being compromised, said the director of the Bureau's regional office.
   Source:
   http://www.suburbanchicagonews.com/couriernews/news/728758,3_1_EL07_A3SCAMS_S1.article

9. *January 6, Bloomberg* – (National) **Securities fraud lawsuits on rise.** Securities fraud class-action suits are on the rise, fueled by subprime mortgage losses, after dropping to a 10-year low in the U.S. in 2006, a study found. Investors sued 166 companies claiming stock fraud in 2007, 43 percent more than the 116 in the prior year, according to a study by the Stanford Law School Securities Class Action Clearinghouse and Cornerstone Research. Six Seattle-area companies were sued by shareholders: Dendreon Corp., Washington Mutual Inc., Jones Soda Co., WSB, Northwest Biotherapeutics, and Zumiez. After remaining low in the first six months of 2007, securities fraud filings accelerated in the second half of the year, according to the study. Of the 100 companies sued in the past six months, 23 were related to subprime losses, the study found, raising the possibility that the increase may not last.
   Source: http://seattlepi.nwsource.com/business/346282_secsuits07.html

[Return to top]

Transportation Sector

10. *January 7, KCRA 3 Sacramento* – (California) **Southwest Jet lands safely after**

emergency. A Southwest Airlines jet landed safely at Sacramento International Airport Monday morning after reporting problems with an engine. The plane, which was not carrying passengers, suffered problems with the left engine, authorities said
Source: http://www.kcra.com/news/14992796/detail.html

11. *January 7, Computer Weekly* – (National) **Concerns over Boeing 'Dreamliner' IT flight systems.** Hackers may be able to access aircraft flight and management systems in Boeing's new mid-range jet, the 787-8, according to the U.S. Federal Aviation Authority. The FAA said that there are links between the networks that run the passenger "domain," which allows passengers to access the internet during flights, and aircraft-management systems. This means they do not contain "adequate or appropriate safety standards for protection and security of airplane systems and data networks against unauthorized access," the FAA said. A Boeing spokesman said the aircraft maker was aware of the problem and would test its fix in March, when the so-called Dreamliner makes its maiden flight. It delayed the first flight in September last year, and postponed deliveries by six months to the end of 2008. At the time it noted an "increasing risk to the delivery schedule," and said "the margin to accommodate unexpected issues had been eliminated."
Source:
http://www.computerweekly.com/Articles/Article.aspx?liArticleID=228784&PrinterFriendly=true

12. *January 6, Boston Globe* – (Massachusetts) **Pilot reports model rocket near airliner.** The pilot of a jet carrying passengers to Logan International Airport reported yesterday that a model rocket appeared to have been fired toward his craft, a Federal Aviation Administration official said. The pilot of AirWisconsin flight 180A saw what appeared to be a spark or firework in front of the plane around 12:26 p.m., after the jet had descended to 500 feet and was preparing to land, said an FAA spokeswoman. The model rocket did not hit the aircraft, she said, and the 40-passenger plane, which had three crew members, landed safely. A State Police spokesman said the plane was flying over the Winthrop-Revere area at the time and the rocket was believed to have been fired from the vicinity of the Belle Isle Marsh Reservation. The state reservation is about a half-mile northeast of two of the airport's runways. State Police are investigating the incident.
Source:
http://www.boston.com/news/local/articles/2008/01/06/pilot_reports_model_rocket_near_airliner/

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture and Food Sector

13. *January 6, Deseret Morning News* – (National) **USU hopes to boost food safety.** Frozen meat lasts longer and is much safer to serve when it can be thawed quickly, according to research being done with a federal grant at Utah State University. “Because meats themselves are most contaminated with potential pathogens,” said a USU extension food safety specialist, who hopes a food safety consortium involving USU and other institutions around the country will be a proper fix for the many organizations that set out to keep food that reaches consumer plates safe. Inspectors, academics, and grocery store managers follow similar protocol, but are not necessarily progressing toward the same goal. Forming a cooperative is one of the main objectives of a $600,000 grant awarded partly to the university earlier this year. The grant is part of $14 million given to researchers and educators at 17 universities for the purpose of improving food safety while reducing the incidence of food-borne illness coming from the million-plus food service establishments across the nation. The consortium will include food safety professionals from five land-grant universities, professional societies, and government agencies that work to put food safely on the table at restaurants or in homes.
    Source: http://deseretnews.com/article/1,5143,695241769,00.html

14. *January 5, Farm and Ranch Guide* – (National; International) **New BSE case in Canada prompts call for USDA to put hold on beef imports.** The announcement by the Canadian government on December 18 that a twelfth case of BSE, commonly known as mad cow disease, had been discovered has prompted two U.S. senators to ask the U.S. Department of Agriculture to suspend a new rule it put into effect less than a month ago which allowed Canadian cattle older than 30 months to be imported into the U.S. The senators requested that such imports be suspended until the USDA fully implements Country-of-Origin Labeling (COOL) for meat sold in the U.S. The senators cited the loss of key export markets due to BSE, saying in a letter to the acting Agriculture Secretary: “Japan and South Korea, formerly the two largest purchasers of U.S. beef, continue to restrict imports in response to the BSE-positive cow found in Washington State that originated in Canada. In the year before this discovery, U.S. beef producers exported 2.52 billion pounds of product worth $3.19 billion. In the following year, this dropped to only 460 million pounds worth $605 million - an astonishing decline of 81 percent!”
    Source:
    http://www.farmandranchguide.com/articles/2008/01/05/ag_news/livestock_news/livestock13.txt

[Return to top]

Water Sector

15. *January 7, Los Angeles Times* – (California) **MWD may cut water to area cities.** In Southern California, the Metropolitan Water District is considering a contingency plan to cut water deliveries to its member cities using a new formula that critics contend favors faster-growing areas while penalizing older, poor communities. The district’s

staff is recommending the plan in case the agency, which serves 18 million people in six counties, is forced to slash water deliveries this spring in the event of continuing shortages. The current discussion signals growing worries that the region's water supplies cannot meet demand, due to last year's record dry weather, an eight-year drought in the Colorado River Basin, and a federal court order last month that sharply reduces water deliveries from Northern California. The proposed formula would determine how much water is allotted to cities and water agencies. Most MWD water is sold to cities at $508 per acre-foot. If a city or agency exceeds its allotment by up to 10 percent, it would be charged a penalty fee of $1,347 per acre-foot. If it uses even more water, the penalty would be higher.
Source: http://www.latimes.com/news/printedition/california/la-me-water7jan07,1,2680454.story?coll=la-headlines-pe-california

16. *January 7, Reuters* – (Michigan) **EPA halts river clean-up talks with Dow Chemical.** The Environmental Protection Agency said Friday it stopped settlement negotiations with Dow Chemical Co., saying the chemical company has not gone far enough in its clean-up plans for a Michigan river. The EPA had previously extended negotiations that began in October in an attempt to reach a final agreement on the clean-up of cancer-causing dioxins from the Tittabawassee River system near Dow's Midland, Michigan, headquarters. "EPA is now reviewing its options for ensuring that dioxin contamination in the river system and the Midland area can be fully addressed," the regional administrator for the EPA said in a statement. Dow responded by saying it was frustrated and disappointed by the decision, noting that agreement on a plan would have resulted in speeding progress toward resolving the situation.
Source: http://www.planetark.org/dailynewsstory.cfm/newsid/46265/story.htm

17. *January 6, Durango Herald* – (Colorado) **Big oil casts big shadow over Colorado's water future.** Stillwater Reservoir, Fourteenmile Reservoir, and Roan Creek Reservoir are all lakes that exist only in the minds of oil company executives and attorneys. The oil companies own legal rights to build and fill these reservoirs, which would be in Colorado's Garfield and Rio Blanco counties. As the companies take another look at Colorado's oil-shale deposits, which would require vast amounts of water to develop, they might make those lakes a reality. Their water rights are huge and getting bigger. Shell has been buying large water rights on the Western Slope for the last five years and just completed a major purchase in July. "I've seen estimates that oil shale, if it is developed, would consume 100 percent of the remaining water in the Colorado River system," said a U.S. senator.
Source: http://durangoherald.com/asp-bin/article_generation.asp?article_type=news&article_path=/news/news080106_4.htm

[Return to top]

Public Health and Healthcare Sector

18. *January 7, Reuters* – (National) **New key to flu's spread discovered.** U.S. researchers have found that that a flu virus must be able to attach itself to an umbrella-shaped receptor coating human respiratory cells before it can infect cells in the upper airways.

The discovery may help scientists better monitor changes in the H5N1 bird flu virus that could trigger a deadly pandemic in humans. And it may lead to better ways to fight it, they said. The H5N1 avian flu virus now almost exclusively infects birds. But it can occasionally pass to a person. Experts have feared that the bird flu virus would evolve slightly into a form that people can easily catch and pass to one another, triggering an epidemic. Before a flu virus can enter a human respiratory cell, a protein on the surface of the virus must bind with chains of sugars called glycans that sit on the outside of the cells. To infect humans, scientists thought the H5N1 bird flu virus would need to simply mutate so it could bind with alpha 2-6 receptors. But it turns out not all alpha 2-6 receptors are the same. Some are short and cone-shaped and some are long and umbrella-shaped. So far, the bird flu virus has found a way to bind only to the cone-shaped structures in human upper airways. The virus has already killed 216 people and infected 348 people in 14 countries, according to the World Health Organization. But the study found that the most infectious human flu viruses bind with the umbrella-shaped receptors in the upper respiratory tract. The researchers believe the H5N1 bird flu virus would need to adapt so it could latch on to these umbrella-shaped receptors before it could be spread readily from human to human.
Source: http://www.msnbc.msn.com/id/22537347/

19. *January 6, HealthDay* – (National) **15,000 toy wagons recalled for too much lead.** Some 15,000 red wagons imported from China by Tricam Industries of Eden Prairie, Minnesota, violate the federal lead paint standard, the U.S. Consumer Product Safety Commission said in announcing the wagons' recall. The recall involves model MH1250. The wagons were sold at Tractor Supply Co. stores across the U.S. from September 2002 through November 2007 for about $30. No injuries have been reported.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2008/01/06/AR2008010600957.html

20. *January 5, KSNW 3 Wichita* – (Kansas) **Virus outbreak leaves Wichita hospitals scrambling to make room.** An outbreak of respiratory syncytial virus (RSV) has Wichita hospitals at capacity. It is a dangerous virus that is causing the worst outbreak Wesley Medical Center has seen in three years. Wesley Medical Center is at capacity withchildren who also have the virus. It is the worst outbreak Wesley has seen in three years. Doctors at Wesley said there is good reason for concern, especially for young children and babies. Via-Christi hospitals have also seen RSV cases double in some of its pediatric units. Wesley is shuffling adult patients to other rooms to make space for all of the sick children. If more come in, Wesley may have to send children miles away for treatment. "Once we've exhausted all of our resources, then we divert to other cities, whether it's Kansas City, Denver or Oklahoma City," said Wesley's Pediatric Manager. That is what Wesley did during the last major outbreak. It could happen again because RSV does not usually peak until February.
Source: http://www.msnbc.msn.com/id/22509947/

21. *January 4, KFOX 14 El Paso* – (Texas) **El Pasoans could wait weeks for medicine in bioterrorism attack.** If something like an anthrax attack or the pandemic flu hits El Paso, Texas, El Paso's Bioterrorism Pandemic Flu Preparedness Program said it will be

mass chaos. The city's department of health will have enough medicine to treat people, but the department said it needs more than 2,000 extra volunteers to give out medicine. As of now the department has about 450 volunteers. At that rate people will be waiting for a long time to get medicine they need. Hospitals will be the first place to fill up if a bioterrorism attack or pandemic flu outbreak happens. That is why the city's health department needs volunteers to run its 29 emergency clinics out of local schools. Right now they can only open about three.
Source: http://www.kfoxtv.com/news/14981114/detail.html

Government Facilities Sector

Nothing to report.

[Return to top]

Emergency Services Sector

22. *January 7, Daily News* – (New York) **FDNY quicker to respond for 3rd year.** The Fire Department of New York's emergency response time has dropped for the third consecutive year -- even as firefighters responded to a record number of calls in 2007, officials said Sunday. It took FDNY units an average of 4 minutes and 49 seconds to reach burning buildings and medical emergencies last year, department brass said. This was as firefighters raced to an all time high 490,767 calls in 2007 -- up 1.2 percent from 484,954 in 2006, officials said. The average response time in 2006 was 4 minutes 54 seconds, down from 5minutes 9 seconds in 2005. The fire commissioner said there was an even bigger drop -- 20 seconds -- in the average response time to the most serious medical emergencies, thanks to new GPS technology in all ambulances in the 911-call system. "With the addition of more advanced training and state-of-the-art equipment in 2007, we have ensured our firefighters and EMS members are better prepared to respond to any crisis, anytime, anywhere," he said. Still, union leaders said the response time to building fires was slower than it was in 2003, when New York City's mayor shut down six engine companies. "It's not all sunshine and roses," said a researcher for the Uniformed Fire Officers Association. The response time to structural fires in 2002 was 4 minutes, 13 seconds, he and FDNY officials said. Last year, it was 14 seconds slower - 4 minutes, 27 seconds. "We're still much slower to fires," he said.
Source: http://www.nydailynews.com/news/2008/01/07/2008-01-07_fdny_quicker_to_respond_for_3rd_year-2.html

23. *January 7, Courier-Journal* – (Kentucky) **Radio system faces final step.** Metro Louisville is about to take its final step in developing a $70 million digital communications system meant to bring all its emergency responders under one umbrella. Construction of three towers, ranging in height from 200 to 500 feet, will begin in April. By summer 2009, MetroSafe's radio system will allow unlimited communication channels for police, firefighters, paramedics, and nonemergency metro government employees. Better communication can help police catch criminals, keep

firefighters from getting lost in smoky buildings, and keep patients alive while being transported to a hospital, first responders say. The system's radio antennas, microwaves and electronic equipment are now being assembled and tested by Motorola, the city's vendor. That equipment should begin arriving in Louisville for assembly in late March, said the Public Works director. The new towers will join nine existing towers that are scheduled for upgrading. In addition, the former Federal Reserve Bank at is being prepared to become the new emergency communications center. The president of the Jefferson County Fire Chief's Association said MetroSafe is important because it will allow firefighters to talk with police and Emergency Medical Services personnel. It will also allow suburban firefighters to communicate with metro Louisville firefighters. Source: http://www.courier-journal.com/apps/pbcs.dll/article?AID=/20080107/NEWS01/801070425

[Return to top]

Information Technology

24. *January 7, IDG News Service* – (International) **CA's website attacked by hackers.** Hackers have attacked software vendor CA's website and are redirecting visitors to a malicious website hosted in China. Although the problem now appears to have been corrected, cached versions of some pages on CA.com show that the site had been redirecting visitors to the uc8010.com domain, which has been serving malicious software since late December, according to the director of the SANS Internet Storm Center. The hack is similar to last year's attack on the Dolphin Stadium website, which infected visitors looking for information on the Super Bowl football game, he said. "It's exactly the same setup," he said. "It's JavaScript that they've managed to insert into the title or the body of the HTML." CA itself may not even host the press release section of its site, as that job is often outsourced to a third party, he said. Often a misconfigured application server or a web or database programming error can give hackers all the opening they need to insert their malicious code. The uc8010.com domain serves attack code that exploits a recently patched vulnerability in the RealPlayer multimedia software, he said. The criminals behind this domain have hacked tens of thousands of Web pages and inserted code that redirects visitors to the malicious server, he added. SANS has posted a note on the uc8010.com issue and recommends that IT staff block access to the domain. He said another domain, ucmal.com, which is also hosted in China, should also be blocked because it is associated with a similar type of attack. Source: http://www.techworld.com/security/news/index.cfm?newsID=11044&pagtype=all

25. *January 7, Computerworld* – (National) **Mass hack infects tens of thousands of sites.** Tens of thousands of Web sites have been compromised by an automated SQL injection attack, and, although some have been cleaned, others continue to serve visitors a malicious script that tries to hijack their PCs using multiple exploits, security experts said this weekend. The chief research officer of Grisoft SRO pointed out that the hacked sites could be found via a simple Google search for the domain that hosted the malicious JavaScript. On Saturday, he said, the number of sites that had fallen victim to the attack numbered more than 70,000. "This was a pretty good mass-hack," he said in a blog post.

"It wasn't just that they got into a server farm, as the victims were quite diverse, with presumably the only common point being whatever vulnerability they all shared." Symantec Corp. cited reports by other researchers that fingered a SQL vulnerability as the common thread. "The sites [were] hacked by hacking robot by means of a SQL injection attack, which executes an iterative SQL loop [that] finds every normal table in the database by looking in the sysobjects table and then appends every text column with the harmful script," said one of the researchers. "It's possible that only Microsoft SQL Server databases were hacked with this particular version of the robot since the script relies on the sysobjects table that this database contains." According to the same researcher, the attack appends a JavaScript tag to every piece of text in the SQL database; the tag instructs any browser that reaches the site to execute the script hosted on the malicious server. Hacked sites included both .edu and .gov domains, added SANS Institute's Internet Storm Center (ISC) in a warning posted last Friday, while others flagged several pages of security vendor CA Inc.'s Web site as infected.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9055858&source=rss_topic17

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Communications Sector

26. *January 5, Government Health IT* – (National) **DHS offers advice for ensuring telecom during pandemic.** The so-called "last mile" of the nation's telecommunications system would be vulnerable in the event of a pandemic influenza, according to a working group tasked with studying the potential communications consequences of an outbreak. The Department of Homeland Security's assistant secretary of cybersecurity and communications weighed in on the security of a pandemic health crisis, noting that as much as 40 percent of the workforce would be unable to go to work during peak periods of an outbreak. "And you don't get to pick which 40 percent that could be," he said during a speech at the New York Metro Infragard Alliance Security Summit in December. "Naturally, telecommuting will be a key mechanism to keeping our businesses and government operational during a pandemic flu." The working group, which meets monthly, found that connections to homes, hospitals, health plans, and physicians would likely be disrupted. But that scenario could be mitigated if ISPs, telecommunications carriers and service vendors put in place safeguards, policies and best practices ahead of time, he said. Among the group's recommendations to hospitals, businesses, and government agencies: obtain a telecommunications service priority (TSP) for enterprises; subscribe to government

emergency telecommunications service (GETS) cards and/or wireless priority services (WPS) capabilities for critical IT staff; limit access to business critical services through the enterprise connection; limit remote access to users critical to maintaining business continuity; adjust or retime automatic desktop backup software updates for telecommuters; and enhance the enterprise's cybersecurity posture due to increased reliance on communications and IT, reduced support staff and the increased threat of cyber attack.
Source: http://www.govhealthit.com/online/news/350155-1.html

[Return to top]

Commercial Facilities Sector

27. *January 6, Associated Press* – (Michigan) **Man walks into Detroit emergency room with grenades, tackled by security.** Detroit Receiving Hospital guards searched a man after he triggered a metal detector Saturday night. An officer found the man had a grenade in one hand with the pin out, the Detroit Free Press reported. The officer tackled him, and the emergency room was evacuated. No injuries were reported. The grenades were a type that might be used in training and much less powerful than combat grenades. Police found two pipe bombs and two grenades in his house. The man, who has a history of mental illness, was hospitalized for evaluation.
Source: http://www.foxnews.com/story/0,2933,320538,00.html

[Return to top]

National Monuments & Icons Sector

28. *January 5, WTNH 8 New Haven* – (Connecticut) **War memorial vandalized again.** For the second time in a week vandals marked up the Vietnam War memorial at Long Wharf in New Haven, Connecticut. This time they did it by spray painting over the names of those who fought and died in the Vietnam War. This is the third time vandals defaced the memorials at the park. White spray paint was cleaned off the memorials stone "V" in early December. Last week, the vandals used bright orange spray paint to write "MS-13". The city is now considering installing cameras at the memorial.
Source: http://www.wtnh.com/Global/story.asp?S=7582672&nav=menu29_2

[Return to top]

Dams Sector

29. *January 7, Providence Journal* – (Rhode Island) **DEM imposes rules for dam inspections.** A recently completed survey of dams in Rhode Island has quadrupled the number considered capable of taking human lives or causing significant economic losses should they fail. The new total of 205 dams considered to pose significant hazards or high hazards is part of a new set of regulations the state Department of Environmental Management recently put into force. More dams are listed either because they were not properly assessed in the past or because new development has placed more people and

property in harm's way should the dams fail. The regulations establish timetables and deadlines for inspecting and repairing dams, particularly those that pose risks to the public. And they are going into effect at the same time that the DEM has intensified its efforts to track down owners of dams that have fallen into disrepair or appear to be abandoned.
Source: http://www.projo.com/news/content/dams_01-07-08_068GC99_v11.2509c5c.html

30. *January 5, Lansing State Journal* – (Michigan) **Report reveals cracks, concrete damage along North Lansing Dam.** In 2009, the Grand River will be lowered to patch the aging North Lansing Dam. Minor cracks and small portions of crumbling concrete were discovered this past summer during an inspection. The resulting report, which reveals no significant problems, was submitted to the state on December 28. The report shows minor cracking, scouring, and weathering of the concrete along the 233-foot-long dam and some of its associated structures. Repairs do not need to be made immediately. The half-inch-thick report by Stantec Consulting Michigan of Ann Arbor suggests some fixes can wait up to four years.
Source:
http://www.lsj.com/apps/pbcs.dll/article?AID=/20080105/NEWS01/801050330/1001/news

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389
Subscription and Distribution Information:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us–cert.gov or visit their Web page at www.us–cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.